**Zamawiający:**

**Powiat Białobrzeski**

**Plac Zygmunta Starego 9**

**26-800 Białobrzegi**

**NIP: 798 14 64 078, REGON: 670223132**

**Załącznik nr 1– Opis przedmiotu zamówienia**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Niniejszy dokument określa szczegółowe wymagania i wytyczne związane z planowanym zakupem usług Pełnomocników (2 osoby) ds. Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostce samorządu terytorialnego (JST) ubiegającej się o grant w Konkursie „Cyberbezpieczny Samorząd” (FERC 2021–2027, Działanie 2.2). Zatrudnienie takiej osoby jest jednym z elementów wzmacniania zdolności JST w obszarze zarządzania ryzykiem, ochrony danych i przeciwdziałania zagrożeniom cybernetycznym.

**I. Rola i zadania Pełnomocnika ds. SZBI**

a) **Koordynacja systemu bezpieczeństwa**  
Pełnomocnik odpowiada za wdrażanie, utrzymywanie i doskonalenie SZBI. Realizuje zadania związane z zapewnieniem zgodności z ustawą o krajowym systemie cyberbezpieczeństwa (uoKSC), Krajowymi Ramami Interoperacyjności (KRI), RODO oraz innymi przepisami prawa i normami (np. ISO/IEC 27001).

b) **Analiza ryzyka i planowanie działań**  
Pełnomocnik we współpracy z działami technicznymi i organizacyjnymi identyfikuje zagrożenia, szacuje ryzyko oraz inicjuje środki zapobiegawcze. Monitoruje również stan bezpieczeństwa, nadzoruje realizację planów ciągłości działania i odpowiada za dostosowywanie urzędu do zmian prawnych.

c) **Współpraca z kadrą zarządzającą i personelem**  
Pełnomocnik jest doradcą kadry zarządzającej i realizuje zadania wykonawcze we współpracy z pracownikami merytorycznymi. Koordynuje wdrażanie wewnętrznych polityk i procedur bezpieczeństwa, a także monitoruje poziom ich przestrzegania.

d) **Komunikacja i raportowanie**  
Pełnomocnik prowadzi kontakty w obszarze bezpieczeństwa informacji, współdziała z zewnętrznymi audytorami oraz właściwymi organami (np. CSIRT). Raportuje do kierownictwa o zagrożeniach, incydentach i postępach w zakresie wdrażania polityk bezpieczeństwa.

**II. Wymagania kompetencyjne i doświadczenie**

a) **Wykształcenie i certyfikacje**

* Co najmniej jeden certyfikat potwierdzający kompetencje w dziedzinie bezpieczeństwa informacji (np. ISO/IEC 27001 Lead Implementer, Audytor wewnętrzny SZBI, CISSP, CISM).
* Minimum 2-letnie udokumentowane doświadczenie we wdrażaniu i nadzorze systemów bezpieczeństwa informacji (np. opracowywanie Polityki Bezpieczeństwa, prowadzenie audytów SZBI, wdrożenia norm ISO/IEC 27001).

b) **Doświadczenie w obszarze cyberbezpieczeństwa**

* Udokumentowany udział w dwóch projektach związanych z podnoszeniem poziomu bezpieczeństwa informacji, w tym w administracji publicznej w przeciągu ostatnich 24 miesięcy.
* Praktyka w analizie i ocenie ryzyka, przeciwdziałaniu incydentom, zarządzaniu kryzysowym i utrzymaniu ciągłości działania.

c) **Znajomość przepisów i wytycznych**

* Krajowe Ramy Interoperacyjności (KRI), ustawa o krajowym systemie cyberbezpieczeństwa (uoKSC), rozporządzenie ws. minimalnych wymagań dla systemów teleinformatycznych oraz RODO.
* Dobre praktyki (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 22301, NIST).

d) **Umiejętności organizacyjne i komunikacyjne**

* Przygotowywanie raportów i komunikacja z kadrą zarządzającą.
* Łączenie zagadnień prawnych i wymagań technicznych z potrzebami administracyjnymi urzędu.

**III. Formuła zatrudnienia i umocowanie w strukturze**

a) **Status Pełnomocnika w urzędzie**

* Bezpośrednie raportowanie do osób z wskazanych w umowie. Obowiązkiem będzie skutecznie inicjować i nadzorować zmiany w obszarze cyberbezpieczeństwa.

b) **Współpraca z zewnętrznym ekspertem**

W sytuacjach, w których konieczne jest przeprowadzenie audytów, weryfikacji lub wdrożeń realizowanych przez zewnętrzne podmioty (np. certyfikowane firmy audytorskie czy doradców w zakresie SZBI), Pełnomocnik ds. SZBI powinien aktywnie współpracować z takimi ekspertami.

**IV. Zakres obowiązków i wskaźniki efektywności**

a) **Podstawowe zadania**

* Opracowywanie planów audytów wewnętrznych i rekomendowanie działań doskonalących bezpieczeństwo informacji.
* Aktualizowanie Polityki Bezpieczeństwa Informacji, w tym procedur dotyczących analizy ryzyka, obsługi incydentów, zarządzania relacjami z dostawcami.

b) **Wskaźniki efektywności**

* Liczba przeprowadzonych testów reakcji na incydenty i sprawdzianów ciągłości działania.
* Skrócenie czasu wykrywania i reagowania na zagrożenia.
* Bieżąca zgodność z wymaganiami KRI, uoKSC oraz innymi wymogami (audytami zewnętrznymi).

c) **Dokumentowanie i raporty**

* Opracowywanie raportów z przeprowadzonych działań i wniosków z audytów.
* Udostępnianie dokumentacji operatorowi projektu i instytucjom kontrolnym w procesie rozliczania środków grantowych.

**V. Uwzględnienie wymagań konkursowych**

a) **Podniesienie dojrzałości cyberbezpieczeństwa**  
Pełnomocnik aktywnie uczestniczy w realizacji zadań w ramach projektu, takich jak audyt SZBI, analiza ryzyka, wdrożenie procedur i zakup narzędzi wspierających bezpieczeństwo.

b) **Zapewnienie zgodności z audytami i rekomendacjami**  
Pełnomocnik odpowiada za współpracę z zespołami wdrożeniowymi oraz zewnętrznymi audytorami, zapewniając dostosowanie procedur urzędu do ewentualnych zaleceń pokontrolnych.

c) **Długoterminowe utrzymanie rezultatów**  
Zadaniem Pełnomocnika jest stałe nadzorowanie, czy wprowadzone w ramach grantu rozwiązania nadal spełniają wymogi prawne i potrzeby organizacyjne, aby zapewnić trwałość efektów po zakończeniu projektu.